E-SHARE EXTERNAL FILE SHARING AND SECURE EMAIL FOR G SUITE

EASY

Nothing to install - As with G Suite apps, there is nothing to install to rollout e-Share to end users. Integration with Google Drive, Google SAML and Gmail allows you to provision e-Share to all end users instantly.

RELIABLE

Private Branding - e-Share allows you to present a private collaboration service to your team, clients, vendors and partners, using your URL, logo, colors, terms of use, etc. Private branding strengthens your brand, instills confidence and trust on the part of those you are collaborating with, and eliminates link blocking.

SECURE

Security & Audit - All files created and uploaded to Google Drive via e- Share are (optionally) encrypted with keys owned by the organization, thereby preventing access to everyone else, including e-Share and Google, to the point where each are unable to fulfill a subpoena to turn over your data.

As the world has moved to more and more mobile computing and ubiquitous connectivity, Google's suite of business productivity tools, re-branded as G Suite in late 2016, has become increasingly more attractive to organizations and businesses of every type and size. Though Google Docs, Sheets and Slides are seeing increasing adoption, the jewels remain Gmail and Google Drive.

Secure Email via Gmail – Initiating a secure email with e-Share can be done right from the familiar Gmail interface or any mail client used by the organization. e-Share's Secure Mail Gateway solution integrates with Gmail to enforce the organization's defined policies as to when an email is processed as a secure email and what access controls the recipient experiences. This unique approach allows the organization and data owners to track each access to secure emails and their attachments, define and extend expiration thresholds, revoke access, etc. With e-Share, a secure email can be the start of a bi-directional collaboration with a recipient, increasing user productivity.

Secure File Storage and Sharing via Google Drive – e-Share's secure collaboration platform can optionally encrypt files to prevent access by Google staff, thereby meeting regulatory requirements for the protection of PII (e.g. HIPAA and GDPR) and ITAR-controlled data. And the links to shared files/folders generated by e-Share are never blocked by the recipient's organization, as is frequently the case with Google Drive alone.

Integration with Google SAML – Organizations leveraging Google as a user identity repository could enable access to e-Share through Google SAML for all or designated employees thus making rollout of the e-Share solution to end users a quick implementation.